Aufgabe 1 (12 Punkte)**.** (a) Zeigen Sie, daß das Polynom $x^7 + 3x + 3 \in \mathbb{Q}[x]$ irreduzibel ist.

(b) Bestimmen Sie die Ordnung der Permutation (12)(34)(567).

(c) Sei G eine abelsche Gruppe und seien $a, b, c \in G$. Angenommen a hat Ordnung 2, b hat Ordnung 4 und c hat Ordnung 6. Bestimmen Sie die Ordnung von $abc \in G$.

(d) Bestimmen Sie alle Einheitswurzeln in dem Körper $\mathbb{Q}(\sqrt{3})$.

Lösung. **Zu (a):** Das angegebene Polynom ist ein Eisensteinpolynom über dem Integritätsring $\mathbb{Z}$ für die Primzahl 3, denn es ist primitiv, und 3 teilt alle Koeffizienten außer den Leitkoeffizienten, und 3^2 teilt nicht den konstanten Term. Damit ist das Polynom irreduzibel über $\mathbb{Z}$ und nach dem Satz von Gauß auch irreduzibel über dem Quotientenkörper $\mathbb{Q}$ von $\mathbb{Z}$.

Zu (b): Der angegebene Zykel $\sigma = (12)(34)(567)$ ist bereits als Zerlegung in disjunkte Zykel dargestellt mit $\sigma_1 = (12)$, $\sigma_2 = (34)$, $\sigma_3 = (567)$. In einem solchen Fall ist die Ordnung von σ genau das kgV der Odnungen von σ_1, σ_2 und σ_3. Da $\operatorname{ord}(\sigma_1) = \operatorname{ord}(\sigma_2) = 2$ und $\operatorname{ord}(\sigma_3) = 3$ ist, folgt $\operatorname{ord}(\sigma) = 6$.

Zu (c): Da G kommutativ ist, gilt wie oben, daß die Ordnung von abc das kgV der Ordnungen von a, b und c ist. Also $\operatorname{ord}(abc) = 12$.

Zu (d): Da $\sqrt{3} \in \mathbb{R}$ gilt $\mathbb{Q}(\sqrt{3}) \subset \mathbb{R}$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, befinden sich alle Einheitswurzeln über $\mathbb{Q}$ in $\mathbb{C}$. Da sie Norm 1 haben, befinden sie sich auf dem Einheitskreis in der komplexen Ebene. Dieser schneidet die reelle Achse in genau zwei Punkten, nämlich $\{1, -1\}$. Diese sind die einzigen Einheitswurzeln in $\mathbb{R}$ und da ebenfalls $\{1, -1\} \subset \mathbb{Q}(\sqrt{3})$ sind dies auch die einzigen EInheitswurzeln von $\mathbb{Q}(\sqrt{3})$.

Aufgabe 2 (12 Punkte)**.** Sei G eine Gruppe.

(a) Sei $H \subseteq G$ eine Ungergruppe von endlichem Index. Zeigen Sie, daß die Menge $\{gHg^{-1} \mid g \in G\}$ endlich ist.

(b) Es seien $n_1, n_2 \in \mathbb{N}$ und es seien $H_1, H_2 \subseteq G$ Unterruppen mit $[G : H_1] = n_1$ und $[G : H_2] = n_2$. (Für eine Untergruppe K von G bezeichne $[G : K]$ den Index von G nach K.) Zeigen Sie, daß $[G : (H_1 \cap H_2)] \leqslant n_1 n_2$ ist.

(c) Sei $H \subseteq G$ eine Untergruppe von endlichem Index. Zeigen Sie, daß ein Normalteiler $N \subseteq G$ von endlichem Index existiert, für den $N \subseteq H$ gilt.

Lösung. **Zu (a):** Betrachte die Abbildung von Mengen

$$G/H \to \{gHg^{-1} \mid g \in G\}, xH \mapsto xHx^{-1}.$$

Diese ist wohldefiniert, denn sei $xH = yH$ für $x, y \in G$, so gilt $y^{-1}x, x^{-1}y \in H$, also

$$xHx^{-1} = xx^{-1}yHy^{-1}xx^{-1} = yHy^{-1}.$$

Es ist klar, daß die Abbildung surjektiv ist. Da $|G/H| = [G : H]$ endlich ist, ist auch $|\{gHg^{-1} \mid g \in G\}|$ endlich.

Zu (b): Betrachte die Abbildung von Mengen

$$G/H_1 \cap H_2 \to G/H_1 \times G/H_2, xH_1 \cap H_2 \mapsto (xH_1, xH_2).$$

Wir zeigen zuerst, daß sie wohldefiniert ist. Sei $xH_1 \cap H_2 = yH_1 \cap H_2$, dann ist $xy^{-1} \in H_1 \cap H_2$, also $xy^{-1} \in H_1$ und $xy^{-1} \in H_2$. Folglich $xH_1 = yH_1$ und $xH_2 = yH_2$ oder zusammen $(xH_1, xH_2) = (yH_1, yH_2)$.
Nun zeigen wir, daß sie injektiv ist. Für zwei Elemente aus dem Bild gelte $(xH_1, xH_2) = (yH_1, yH_2)$. Es folgt $xH_1 = yH_1$ und $xH_2 = yH_2$, also $xy^{-1} \in H_1$ und $xy^{-1} \in H_2$. Zusammen $xy^{-1} \in H_1 \cap H_2$ und das bedeutet $xH_1 \cap H_2 = yH_1 \cap H_2$.

Für die Mächtigkeit von $G/H_1 \cap H_2$ können wir nun schließen

$$[G : H_1 \cap H_2] \leqslant |G/H_1 \times G/H_2| = |G/H_1| \cdot |G/H_2| = n_1 \cdot n_2.$$

Zu (c): Die Teilmengen $gHg^{-1} \subset G$, wobei g die Elemente von G durchläuft sind die zu H konjugierten Untergruppen. Nach (a) gibt es davon endlich viele. Setze

$$N := \bigcap_{g \in G} gHg^{-1}.$$

Als Schnitt von Untergruppen ist dies wieder eine Untergruppe. Weiterhin gilt für $x \in G$

$$xNx^{-1} = \bigcap_{g \in G} xgHg^{-1}x^{-1} = \bigcap_{y=xg, g \in G} yHy^{-1} = \bigcap_{y \in G} yHy^{-1},$$

wobei die letzt Gleichhit gilt, da die Multiplikation mit x bijktiv auf G ist. Also ist N wirklich ein Normalteiler von G (und amit auch von H. Für alle Gruppen gHg^{-1} gilt $[G : gHg^{-1}] = [G : H] = n$. Wir wenden Teil (b) induktiv auf den endlichen Schnitt $\bigcap_{g \in G} gHg^{-1}$ an und erhalten

$$[G : N] \leqslant [G : H]^m,$$

wobei m die Anzahl der verschiedenen Untergruppen $gHg^{-1} \subset G$ ist.

Aufgabe 3 (12 Punkte)**.** Seien p eine Primzahl, $q = p^n$ $(n \geqslant 1)$ eine Primzahlpotenz und $\mathbb{F}_q$ der endliche Körper mit q Elementen.

(a) Zeigen Sie im Falle $p \neq 2$: $|\{x^2 \mid x \in \mathbb{F}_q\}| = \frac{q+1}{2}$

(b) Sei $\alpha \in \mathbb{F}_q$ gegeben. Zeigen Sie, daß $x, y \in \mathbb{F}_q$ so existieren, daß $\alpha = x^2 + y^2$ gilt.
Hinweis: Betrachten Sie den Schnitt der Mengen $\{\alpha - x^2 \in \mathbb{F}_q \mid x \in \mathbb{F}_q\}$ und $\{y^2 \in \mathbb{F}_q \mid y \in \mathbb{F}_q\}$.

Lösung. **Zu (a):** Natürlich ist 0 ein Quadrat in $\mathbb{F}_q$. Es bleibt also die Anzahl der Quadrate in der multiplikativen Gruppe $\mathbb{F}_q^*$ zu bestimmen. Betrachte hierauf den Gruppenhomomorphismus

$$\psi : \mathbb{F}_q^* \to \mathbb{F}_q^*, x \mapsto x^2.$$

Sein Bild $\operatorname{im}(\psi)$ sind genau die Quadrate ungleich Null in $\mathbb{F}_q$. Der Kern ist

$$\ker(\psi) = \{x \in \mathbb{F}_q^* \mid x^2 = 1\}.$$

Dies sind genau die Nullstellen des Polynoms $X^2 - 1 \in \mathbb{F}_q[X]$. Da $p \neq 2$, ist in $\mathbb{F}_q$ $1 \neq -1$, also ist $\ker(\psi) = \{1, -1\}$. Nach dem Homomorphiesatz induziert ψ einen Isomorphismus

$$\mathbb{F}_q^* / \ker(\psi) \xrightarrow{\sim} \operatorname{im}(\psi).$$

Nach dem Satz von Lagrange ist

$$|\operatorname{im}(\psi)| = |\mathbb{F}_q^*| : |\ker(\psi)| = \frac{q-1}{2}.$$

Also gibt es $\frac{q-1}{2}$ Quadrate in $\mathbb{F}_q^*$. Zusammen mit der Null also $\frac{q+1}{2}$ Quadrate in $\mathbb{F}_q$.

Zu (b): Sei $M_1 = \{\alpha - x^2 \in \mathbb{F}_q \mid x \in \mathbb{F}_q\}$ und $M_2 = \{y^2 \in \mathbb{F}_q \mid y \in \mathbb{F}_q\}$. Wir haben bereits festgestellt, daß M_2 die Mächtigkeit $\frac{q+1}{2}$ hat. Betrachte nun die Abbildung

$$M_2 \to M_1; u \mapsto \alpha - u.$$

Diese ist eine bijektive Abbildung von Mengen. Also hat die Menge M_1 ebenfalls $\frac{q+1}{2}$ Elemente. Es gilt $M_1 \cup M_2 \subset \mathbb{F}_q$. Wäre der Schnitt von M_1 und M_2 leer, dann wäre

$$q + 1 = |M_1 \cup M_2| \leqslant |\mathbb{F}_q| = q.$$

Ein WIderspruch. Also enthält der Schnitt $M_1 \cap M_2$ Mindestens ein Element u, das heißt es gibt $x, y \in \mathbb{F}_q$ mit $\alpha - x^2 = u = y^2$. Für diese gilt also $\alpha = x^2 + y^2$.

Aufgabe 4 (12 Punkte)**.** Seien $p > 0$ eine Primzahl, $\mathbb{Q} \subseteq K$ eine Körpererweiterung vom Grad p, $\alpha \in K$ ein Element mit $K = \mathbb{Q}(\alpha)$, $\alpha_1 = \alpha, \ldots, \alpha_p$ die Konjugierten von α über $\mathbb{Q}$ und letztlich $E := \mathbb{Q}(\alpha_1, \ldots, \alpha_p)$ die normale Hülle von $K/\mathbb{Q}$.

(a) Zeigen Sie, zum Beispiel durch Betrachten der Operation der Galoisgruppe auf den Nullstellen, daß die Galoisgrippe $\mathrm{Gal}(E/\mathbb{Q})$ eine zyklische Untergruppe der Ordnung p enthält.

(b) Zeigen Sie: Gilt $\alpha_2 \in K$, so folgt $K = E$.

Lösung. **Zu (a):** Nach Voraussetzung ist $[K : \mathbb{Q}] = p$ und nach dem Gradsatz

$$[E : \mathbb{Q}] = [E : K] \cdot [K : \mathbb{Q}]$$

also $p \big| [E : \mathbb{Q}]$. Da aber $E/\mathbb{Q}$ eine Galoiserweiterung ist (denn sie ist normal, und da $\mathbb{Q}$ Charakteristik 0 hat auch separabel), gilt

$$[E : \mathbb{Q}] = |\,\mathrm{Gal}(E/\mathbb{Q})|,$$

also teilt p die Mächtigkeit von $\mathrm{Gal}(E/\mathbb{Q})$ Nach dem Satz von Cauchy enthält $\mathrm{Gal}(E/\mathbb{Q})$ ein Element σ der Ordnung p. Die davon erzeugte Untergruppe $P := \langle\sigma\rangle \subset \mathrm{Gal}(f/\mathbb{Q})$ ist eine zyklische Gruppe der Ordnung p.

Zu (b): Sei f das Minimalpolynom von α. Die Konjugierten zu α sind genau die Nullstellen von f. Nach Voraussetzung ist E ein Zerfällungskörper von f und nach Definition $\mathrm{Gal}(f/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q})$. Wir betrachten nun die Operation der Gruppe $G = \mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(f/\mathbb{Q})$ auf die Nullstellenmenge $\{\alpha_1, \ldots, \alpha_p\}$ Da f irreduzibel ist, ist die Operation transitiv. Für α_i sei G_{α_i} die STabilisatoruntergruppe. Ist $\alpha_2 \in \mathbb{Q}(\alpha_1)$, so ist $G_{\alpha_1} \subset G_{\alpha_2}$. Da die Operation transitiv ist, sind die Stabilisatoruntergruppen gleichmächtig, also folgt $G_{\alpha_1} = G_{\alpha_2}$.
Betrachte nun die Menge $M = \{G_{\alpha_1}, \ldots, G_{\alpha_p}\}$ deren Elemente die Stabilisatoruntegruppen der α_i sind. Da $G_{\alpha_1} = G_{\alpha_2}$ gilt $|M| < p$. Die p-Gruppe P aus (a) operiert auf M durch Konjugation

$$P \times M \to M, (g, G_{\alpha_i}) \mapsto gG_{\alpha_i}g^{-1}$$

denn $gG_{\alpha_i}g^{-1} = G_{g\alpha_i}$. Da P transitiv auf die Nullstellen operiert, ist uach diese operation transitiv, und damit $|M| \;\big|\; |P| = p$, also muß $|M| = 1$ und damit stimmen alle Stabilisatoruntergruppen überein. Da $G_{\alpha_i} = \mathrm{Gal}(E/\mathbb{Q}(\alpha_i))$ stimmen also alle $\mathrm{Gal}(E/\mathbb{Q}(\alpha_i)$ überein. Nach dem Hauptsatz der Galoistheorie stimmen damit alle $\mathbb{Q}(\alpha_i)$ überein. Insbesondere $\alpha_i \in K$ für alle $1 \leqslant i \leqslant p$, das heißt $K = E$.

Aufgabe 5 (12 Punkte)**.** Sei $K = \{0, 1, a, b\}$ ein Körper mit vier Elementen (0 sei das Nullelement, 1 das Einselement).

(a) Stellen Sie die Additions- und die Multiplikationstabelle von K auf.

(b) Sei $f(X) = X^4 + X + 1 \in K[X]$. Zeigen Sie, daß f reduzibel ist.

(c) Bestimmen Sie den Grad des Zerfällungskörpers von f über K.

Lösung. **Zu (a):** Additionstabelle:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Multiplikationstabelle:

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Zu (b): Das Polynom f hat keine Nullstelle in K:

$$
\begin{aligned}
f(0) &= 1 \\
f(1) &= 1 \\
f(a) &= a^4 + a + 1 = b^2 + a + 1 = 2a + 1 = 1 \\
f(b) &= b^4 + b + 1 = 1
\end{aligned}
$$

Also spaltet es keinen Linearfaktor ab. Es zerfällt in quadratische irreduzible Polynome in $K[X]$

$$X^4 + X + 1 = (X^2 + X + a)(X^2 + X + b).$$

Zu (c): Sei $f_a = X^2 + X + a$ und $f_b = X^2 + X + b$. Sei α eine Nullstelle von f_a. Wie man leicht sieht ist $\alpha + 1$ die zweite Nullstelle. also $f_a = (X + \alpha)(X + \alpha + 1)$. Der Zerfällungskörper von f_a ist $K(\alpha)$ und hat Grad 2.
Weiterhin ist $\beta = \alpha + a$ eine Nullstelle von f_b:

$$f_b(\alpha + a) = (\alpha + a)^2 + \alpha + a + b = \alpha^2 + \alpha + a^2 + a + b = \alpha^2 + \alpha + a = f_a(\alpha) = 0$$

Die zweite Nullstelle von f_b ist wiederum $\beta + 1 = \alpha + a + 1$. Die vier Nullstellen von f sind also $\{\alpha, \alpha + 1, \beta, \beta + 1\}$ und f zerfällt über $K(\alpha)$ in die Linearfaktoren

$$f = (X + \alpha)(X + \alpha + 1)(X + \beta)(X + \beta + 1).$$

Damit ist $K(\alpha)$ der Zerfällungskörper von f und $[K(\alpha) : K] = 2$.